代数幾何符号の歩み (符号と暗号の代数的数理)

AUTHOR(S):

水野, 弘文

CITATION:

水野, 弘文. 代数幾何符号の歩み (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 143-151

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25267

数理解析研究所講究録 1361 巻 2004 年 143-151

代数幾何符号の歩み

イオンド大学　　水野弘文 (Hirobumi Mizuno)
Iond University

1 序

代数幾何学と符号理論は、長い間互いに無関係にそれぞれ独自の発展を遂げつつあった。ところが、1980 年頃になって Goppa は代数曲線と符号との間に深い関係があるという事実に気がついて、代数曲線の性質を利用して効率のよい誤り訂正符号を構成することを考えた。また、代数幾何学において取扱われる種々の概念と、符号理論における諸概念との間の対応を明らかにし、代数幾何学における定義や定理をいわば符号理論の言葉に翻訳した。このあたりのことを理解するためには、あらかじめこれら二つの言語をある程度知っていることが必要であろう。

代数幾何学は、数世紀にわたる歴史をもつ数学の一分野である。一方、符号理論を含む情報理論の研究の出発点は

Shannon,C.E., A Mathematical Theory of Communication, Bell System Tech. J. (1948)

であり、比較的新しい研究分野である。1950 年に Hamming 符号が発見され、1960 年頃には BCH 符号や Reed-Solomon 符号が考案された。1970 年には、 Goppa が論文

Goppa, V.D., A new class of linear error-correcting codes

を発表し、有理式を用いる新しい符号を定義した。この符号は古典 Goppa 符号と呼ばれるようになる。そして、1980 年頃に彼が考え始めた代数幾何符号のプロトタイプになっている。

2 代数幾何学の歴史

代数幾何符号の理論において、中心的な役割を果たすのは、代数曲線に対する Riemann - Roch の定理であろう。そこで、代数曲線の理論の発展について簡単に復習しておこう。

2.1 複素関数論と Riemann

Abel と Jacobi は、楕円曲線とその上の積分、すなわち楕円積分、そしてその逆関数である楕円関数について一般的理論を建設した。その結果は、Göpel と Rosenhein によって種数 2 の場合に拡張された。Weierstrass は種数 $g \geq 2$ の超楕円曲線の場合に Jacobi の逆問題を解決した。それに続いて、Riemann は 1857 年の論文 "Theorie der abelischen Functionen" において最も一般的な場合に Jacobi の逆問題を完全に解決した。また、Riemann-Roch の定理のうちの Riemann Part と呼ばれる不等式の部分を与えた。これはそのあと Riemann の弟子の一人である Roch により等式の形に完成される。Riemann の研究の出発点は代数曲線に対応する閉 Riemann 面、すなわちコンパクトな 1 次元複素多様体であり、その方法は Riemann 面上の abel 積分である。閉 Riemann 面は位相幾何学的には、向きづけ可能な閉曲面である。その 1 次元 Betti 数を b_1 とするとき、$g = \frac{1}{2}b_1$ によってこの Riemann 面、あるいはそれに対応する代数曲線の種数が定義される。

2.2 Max Noether と代数幾何学

V.D.Goppa は代数幾何符号についての 1983 年の論文:"Algebraico-geometric codes, Math. USSR. Izvestia 21 " において、A.Brill - M.Noether の考え方に沿って，代数曲線上の線形系 (linear series) の言葉を用いて彼自身の与えた結果を述べている。そして、代数幾何学を符号理論に応用しようとする者にとって、古典的テキスト:" F.Severi : Vorlesungen über algebraische Geometrie, 1921 " が最も適当であると書いている。この小論ではなるべく Goppa の立場を尊重することにし、Goppa の論文を読む場合に役に立ちそうな事柄を簡単にまとめておくことにしよう。

方程式

$$f(X, Y) = 0$$

で与えられる平面代数曲線 C の次数が m とする。C の 1 点 P が r 重点で、P において r 本の異なる接線がひけるとき、P は C の通常 r 重点と呼ばれる。さて、曲線 C が点 $P_1, \cdots, P_k$ においてそれぞれ $r_1, \cdots, r_k$ 重の通常特異点をもち、それ以外は特異点をもたないとする。もし C が既約ならば、

$$g = \frac{1}{2}(m-1)(m-2) - \sum_{i=1}^{k} \frac{1}{2} r_i(r_i - 1)$$

は非負の整数になることが示される。この g を代数曲線 C の種数 (幾何種数) と呼ぶ。それは、C に対応する Riemann 面の位相幾何学的種数と等しいことが示される。

各 r_i $(1 \leq i \leq k)$ 重点 P_i で少なくとも重複度 $r_i - 1$ をもつ曲線を C の随伴曲線 (adjoint curve) という。特に、次数が $m-3$ の随伴曲線は特殊随伴曲線 (special adjoint curve) と呼ばれる。$g \gg 1$ ならば、C の特殊随伴曲線で線形独立なものが g 個存在する。

$$C' : \phi(X, Y) = 0$$

を 1 つの特殊随伴曲線としよう。このとき

$$\omega = \frac{\phi(X, Y)}{f_Y(X, Y)} dX$$

は C 上の第 1 種微分を与える。

C' が C と交わるとき、その $P_1, \cdots, P_k$ 以外での交点の集合は曲線 C の因子を定める。重複度も含めて考えることにすると、このようにして得られる因子は次数 $2g-2$ をもつ。この因子 W は C の標準因子 (canonical divisor) である。C の標準因子の全体は $g-1$ 次元の完備線形系 (complete linear series) $|W|$ をなす。

曲線 C 上に因子 D が与えられたとき、D の成分である C の各点を (重複度も考慮して) 通る特殊随伴曲線がもう 1 つ存在するならば、因子 D は特殊 (special) であると言う。そのような特殊随伴曲線全体のつくるベクトル空間の次元を $i(D)$ と表し、因子 D の特殊指数 (speciality index) と呼ぶ。曲線 C 上の有理関数の集合

$$L(D) = \{f : (f) + D \geq 0\} \cup \{0\}$$

は有限次元ベクトル空間になる。その次元を $l(D)$ と表すとき、我々が必要とする Riemann-Roch の定理は

$$l(D) = \deg D - g + 1 + i(D)$$

で与えられる。また

$$i(D) = l(W - D).$$

2.3 代数的方法

Riemann の思想を純代数的に再構成しようと試みたのは Kronecker および Dedekind である。Kronecker は数論と代数幾何学を共に含む壮大な統一理論を構想していたと思われる:

Kronecker,L.:Grundzüge einer arithmetischen Theorie der algebraischen Grössen, Crelle 92,1882
しかし、それの実現のためには、Zariski, Weil, Serre らによる可換環その他の理論、そして Grothendieck によるスキームの理論を持たなければならなかった。

Dedekind は、あたえられた Riemann 面上の有理関数全体のつくる体と、有限次代数体との間に見られる類似性に着目し、Riemann の考えを、数論の方法を用いて純代数的に再構成した。

Dedekind,R. - Weber,H. :Theorie der algebraischen Funktionen einer Veräuderlichen, Crelle 92,1882

この理論は、Hensel,K., Landsberg, G., Schmid,F.K. らに引き継がれ

Chevalley,C.:Introduction to the theory of algebraic functions of one variable, AMS. Math. Surveys, 1951
において読みやすい形で展開されている。この本は最近の符号理論の文献でも引用されることが多い。同じく数論的立場から Stichtenoth が次の本を著している:

Stichtenoth,H.:Algebraic function fields and codes, Springer, 1993
ただし、この方向の理論における研究の対象はあくまでも代数関数体であって、幾何学的概念である代数曲線は表面には現れない。代数幾何学とは関係ないところで展開された理論を用いて構成された符号を代数幾何符号と呼ぶのが適切であるのかどうか、少々気になる点ではある。

Goppa は先に触れた論文

Goppa,V.D.:Algebraico-geometric codes, Math. USSR Izvestia, 1983
において、代数曲線の代わりに任意次元の代数多様体を用いて符号を定義することができること、そして一例として、Veronese 多様体から得られる符号が Muller 符号と一致することに注意している。ところで、1 次元の場合には代数関数体の理論の枠の中で Riemann-Roch の定理、留数定理など符号理論に必要な結果を全て導き出す事ができる. しかし、代数曲面を含む高次元代数多様体については、関数体の理論の中だけで研究を進めることは出来ない。要するに、代数幾何学を避けて代数幾何符号を構成することは不可能である。

3 代数幾何符号

代数幾何符号の創始者である V.D.Goppa の業績についてあらためて考察することにしよう。

3.1 古典 Goppa 符号

Goppa は 1870 年の論文

A new class of linear error-correcting codes

において新しい符号 $\Gamma(L,g)$ を提案した。それは、次のように定義される。$L := \{\gamma_0, \gamma_1, \cdots, \gamma_{n-1}\}$ を $\mathbf{F}_{q^m}$ の n 個の元の集合とし、$g(z) \in \mathbf{F}_{q^m}[z]$ はモニック多項式で、$g(\gamma_i) \neq 0,\ 0 \leq i \leq n-1$ とする。このとき

$$\Gamma(L,g) := \left\{ (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}_q^n : \sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} \equiv 0 \mod g(z) \right\}.$$

$\Gamma(L,g)$ は $g(z)$ を Goppa 多項式とする古典 Goppa 符号と呼ばれる。

射影直線上の微分

$$\omega = \sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} dz$$

は高々点 $z=\gamma_i$ で 1 位の極をもつ第 3 種微分で、そこでの留数は c_i である。ただし $0 \leq i \leq n-1$. 無限遠点 ∞ での局所変数を $u := \frac{1}{z}$ とすると、$dz = -\frac{1}{u^2}du$ であるから、$z=\infty$ の近傍では

$$\omega = -\sum_{i=0}^{n-1} \frac{c_i}{1-\gamma_i u} \cdot \frac{1}{u} du$$

と表わせる。ω は無限遠点で 1 位の極を持ち、そこでの留数 c_n は $c_n = -\sum_{i=0}^{n-1} c_i$ で与えられる。ベクトル

$$\boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1}, c_n)$$

は、写像

$$\varphi_\Omega : \omega \longmapsto (\mathrm{Res}_{\gamma_0}\omega, \mathrm{Res}_{\gamma_1}\omega, \cdots, \mathrm{Res}_{\gamma_{n-1}}\omega, \mathrm{Res}_\infty \omega)$$

による ω の像になっている。$\mathrm{Im}\ \varphi_\Omega$ は $\mathbf{F}_q^{n+1}$ の部分空間であり、それは $\Gamma(L,g)$ の拡大符号 (extended code) になっていることに注意しよう。

3.2 代数曲線上の符号

先の論文を発表してから約 10 年後、Goppa は論文

Codes on algebraic curves, Soviet Math, Dokl.,1981

において代数幾何符号 $\Gamma(D,G)$ を定義し、以下に述べる事柄を示した。

C を有限体 $\mathbf{F}_q$ 上定義された種数 g の射影曲線とする。$P_1, \cdots, P_n$ を C の $\mathbf{F}_q$ 有理点とし、正因子 $D = \sum_i P_i$, $G = \sum m_Q Q$ を考える。G は $\mathbf{F}_q$ 有理的因子で、D と共通の成分は持たないと仮定する。すなわち $\mathrm{supp}\, D \cap \mathrm{supp}\, G = \phi$. 微分 ω の因子を (ω) と表すとき、$\mathbf{F}_q$ 上定義される C の上の微分で $(\omega) \geq G - D$ となるものの全体は $\mathbf{F}_q$ 上の有限次元ベクトル空間になる。それを $\Omega(G-D)$ とかく。線形写像

$$\varphi_\Omega : \Omega(G-D) \longrightarrow \mathbf{F}_q^n$$

$$\varphi_\Omega(\omega) = (\mathrm{Res}_{P_1}(\omega), \cdots, \mathrm{Res}_{P_n}(\omega))$$

を考える。このとき、$\mathrm{Im}(\varphi_\Omega)$ を $\Gamma_\Omega(D,G)$ と表して、それを微分型の (D,G) 符号という。もし

$$2g - 2 < \deg G < n$$

ならば、$\Gamma_\Omega(D,G)$ の次元 k, 最小距離 d は関係

$$k = n - \deg G + g - 1$$

$$d \geq \deg G - 2g + 2$$

を満たすことが、Riemann-Roch の定理を用いることによって容易に導かれる。それは、射影直線上の符号である古典 Goppa 符号の拡大符号の自然な一般化になっていることがわかる。

3.3 Modular 曲線と代数幾何符号

すでに 1982 年の論文

Tsfasman,M.A., Vladut,S.G., and Zink,Th., Modular curves, Shimura curves, and Goppa codes, better than Varshamov - Gilbert bound, Math.Nach.,109

において、modular 曲線を用いて、$q = p^{2n} > 49$ の場合 VG 限界を越える q 元代数幾何符号の無限列が存在することが示されている。

Goppa は 1988 年に

Geometry and codes, Kluwer Academic Publishers

という本を書いている。そして Hamming 符号、BCH 符号、RS 符号などについても幾何学的な立場からそれらを眺めている。そして有理点をたくさん含む代数曲線を構成する方法として modular 曲線や、代数曲線の被覆曲線や、代数曲線の被覆曲線が有効であると述べている。

modular 曲線は数論、代数幾何学の分野で中心的な研究題目の一つであるが、符号理論の立場からも更に進んだ研究が期待される。

符号理論の研究者のための代数幾何および modular 曲線への入門書としては

Moreno,C.:Algebraic curves over finite fields, Cambridge University Press, 1991

がある。

4 代数幾何符号の復号法

S.Sakata は、もともと代数幾何符号とは関係のない立場で Berlekamp-Massey のアルゴリズムを高次元の場合に拡張する研究を行っていたが、J.Justesen らはこの Sakata アルゴリズムを代数幾何符号の復号に応用した。

J.Justesen, K.J.Larsen, H.Elbrϕnd Jensen, and T.Hϕholdt, Fast decoding of codes from algebraic plane curves, IEEE Trans. Information Theory, **38**(1992)

この方向の研究はその後 G.- L. Feng and T.R.N.Rao や S.Sakata らによってさらに発展している。

5 ゼータ関数と符号理論

ゼータ関数は不思議な魅力的な研究対象で、いろいろな種類がある。Riemann のゼータ関数に関する予想はまだ未解決である。Goppa は先に引用した本の中で、代数曲線のゼータ関数を紹介している。そして、代数曲線の有理点の個数を評価する Hasse-Weil の限界式に触れている。ゼータ関数は数論や代数幾何学だけでなく、グラフ理論、不連続群などの分野にも登場するが、最近は符号理論においてもゼータ関数が導入され、今後の展開が注目される。

6 高次元代数多様体、特に代数曲面から生成される代数幾何符号

代数曲線から得られる代数幾何符号について振り返ってみると、曲線の種数 g が 0, すなわち有理曲線の場合には Reed-Solomon 符号または古典 Goppa 符号が出てくるだけで、特に真新らしいものはない。興味ある符号が得られるのは $g \geq 1$ の場合である。

代数曲面から作られる符号についても同様の事情が生じていると思われる。そこで、まず代数曲面の種数について述べる。

6.1 代数曲面の不正則数

Riemann は代数曲線の種数 g を、対応する Riemann 面の 1 次元 Betti 数 b_1 を用いて $g = \frac{1}{2}b_1$ と定義した。曲線の標準因子を W とすれば

$$g = l(W)$$

であり、曲線の次数が m なら、$m-3$ 次の随伴曲線で線形独立なものの最大個数、あるいは、第 1 種 abel 微分で線形独立なものの最大個数である。

代数曲面の場合にも、それに対応する複素解析曲面の 1 次元 Betti 数を b_1 とすれば、$r = \frac{1}{2}b_1$ は、この曲面上の単純第 1 種微分 (Picard 微分) で線形独立なものの最大個数になる。考えている曲面が 3 次元射影空間の中の非特異代数曲面の場合には $r = 0$ となることが知られている。

6.2 幾何種数

代数曲面 S の標準因子を W と表すとき

$$P_g = l(W)$$

は S の幾何種数と呼ばれる。それは S 上の第 1 種 2 重微分で線形独立なものの最大個数に等しい。S が $\mathbf{P}^3$ の中の m 次代数曲面で、通常特異点だけを持つとする。すなわち、S の 2 重曲線 Γ は既約で、その次数は n, 種数は P そして t 個の 3 重点をもつとする。Γ を通る $\mathbf{P}^3$ の中の曲面を S の随伴曲面と呼ぶ。特に、$m-4$ 次の随伴曲面で線形独立なものの最大個数が P_g である。

6.3 算術種数

m 次平面代数曲線 C が d 個の通常 2 重点をもつとき曲線 C の種数は

$$g = \binom{m-1}{2} - d$$

であった。

m 次曲面 $S \subset \mathbf{P}^3$ が 6.2 で述べたように特異点をもつとき、十分大きい正整数 l に対して、S の l 次随伴曲面で線形独立なものの最大個数は l の 3 次多項式

$$\varphi(l) = \binom{l-1}{3} - n(l-4) + 2t + P - 1$$

で与えられる。$l = m-4$ のときこの式が $m-4$ 次随伴曲面で線形独立なものの最大個数 P_g を与えてくれれば曲線の場合と同様に簡単であるが、一般にはそれらは等しくない。そして、

$$P_a = \varphi(m-4)$$

に対して不等式 $P_a \leq P_g$ が成り立つ。しかも、それらの差は 6.1 で述べた不正則数 q に等しい:

$$P_g - P_a = q$$

6.4 代数曲面から構成される符号

代数曲面の性質を用いて効率のよい符号を構成しようと思えば、不正則曲面、すなわち

$$P_g - P_a = q > 0$$

を満たす曲面の理論、しかも有限体上で定義された代数曲面の理論を構築する必要がある。また、代数曲線の場合と同様に、2 変数 modular 関数の理論も重要になるであろう。

さて、S から導かれる微分型符号を構成するためには、S 上の第 3 種単純微分および 2 重微分に対して、それらが極としてもつ S 上の曲線に沿っての留数の概念を明確にし、それらの性質を有限体の場合に明らかにしなければならない。

代数曲線の場合には、関数型符号と微分型符号とは互いに双対であることが留数定理から直ちに導かれる。代数曲面、そして高次元多様体の場合には、関数型の符号は容易に構成できる。そして、その双対符号ももちろん線形符号にはちがいない。しかし、その代数幾何学的意味は不明である。微分やその留数と関係があるのかないのかもわからない。したがってその辺の事情が明らかにならない限り、関数型符号の双対符号を微分型符号と呼ぶわけにもいかない。